Управление информационной безопасностью в среде виртуализации VMware

Текущее состояние, проблемы и перспективы развития

Мария Сидорова

VMUG, Москва, 26 июня 2009

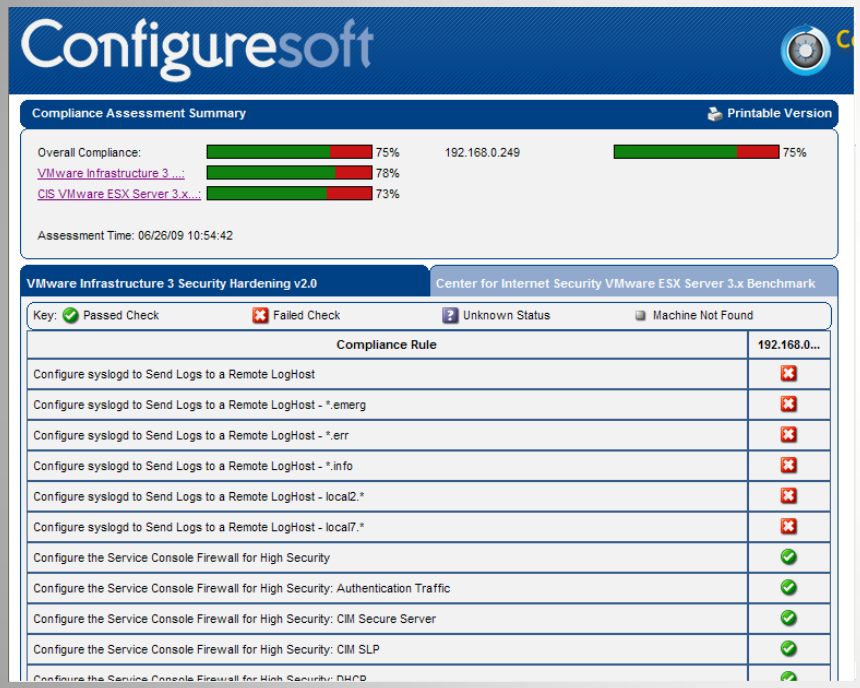
Поговорим о…

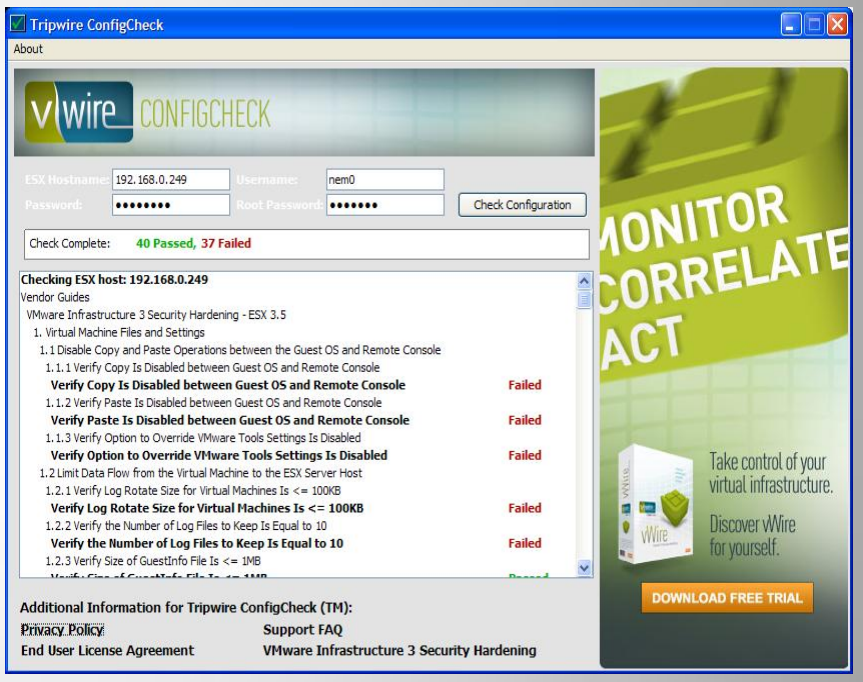
- Плюсах и минусах документов по обеспечению информационной безопасности компании VMware;
- Проблемах, которые возникают при разработке концепций информационной безопасности для инфраструктуры виртуализации;
- Перспективах развития обеспечения информационной безопасности инфраструктуры виртуализации.

Best-practice

- VMware Infrastructure 3.5 Security Hardening (VMware);
- VMware ESX server 3.x Benchmark (CIS);
- VMware ESX server in the Enterprise Planning and securing virtualization servers (Edvard L. Haletky);
- VMware Virtual Infrastructure3 Security Risk Assessment (Xtravirt).

Экспресс-анализ ESX-серверов





АЛМИТЕК

Уровни безопасности

- Уровень виртуализации (VMKernel и монитор виртуальной машины);
- Виртуальные машины;
- Сервисная консоль сервера ESX;
- Сервер ESX (уровень виртуальной сети);
- Сеть хранения данных;
- Сервер управления инфраструктурой Virtual Center.

VMware Virtual Infrastructure3 Security Risk Assessment (Xtravirt).

Реагирование на инциденты

- Скомпрометирована виртуальная машина;
- Скомпрометирован отдельный сервер ESX;
- Скомпрометирован ESX сервер кластера;
- Скомпрометирован Virtual Center.

Перспективы развития

- Разработка продуктов и технологий обеспечения информационной безопасности инфраструктуры виртуализации;
- Консолидированные усилия специалистов и сообщества пользователей продуктов VMware, направленные на противодействие угрозам в среде виртуализации.

Skype: m.e.sidorova

Email: sidorova@almitech.ru

Мария Сидорова

Москва, 26 июня 2009

АЛМИТЕК